



MoGua

PH 1.1.1.APK 分析报告



APP名称:

PH

包名: com.phppx.ppxone2sdf2s3f2390528

域名线索: 45条

URL线索: 19条

邮箱线索: 3条

分析日期: 2025年6月14日

分析平台: [摸瓜APK反编译平台](#)

文件名: ph114dh001_2025.6.11.400.apk
文件大小: 23.64MB
MD5值: a25d3cbe9a13ad51fedcc5d36ae0a2f7
SHA1值: 11e3a27676631c66111b3f4b2690ad57881e0ed2
SHA256值: c814d6e5adccf5d7e335ef95251acd3c7f28c58d3498ca06df84c1791e6d17bf

i APP 信息

App名称: PH
包名: com.phppx.ppxone2sdf2s3f2390528
主活动Activity: com.zq.douyin.MainActivity
安卓版本名称: 1.1.1
安卓版本: 3

🔍 域名线索

域名	服务器信息
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
img01.yzcdn.cn	IP: 27.222.18.107 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
swiperjs.comn	没有服务器地理信息.
	IP: 118.107.9.213

spark.hzo732.com	所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
dzu541irseb11.cloudfront.net	IP: 3.166.243.48 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
issues.apache.org	IP: 168.119.33.54 所属国家: Germany 地区: Bayern 城市: Gunzenhausen 纬度: 48.323860 经度: 11.601019
axios-http.com	IP: 52.76.120.174 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
hfive.qsxon.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
leg.rym508.com	IP: 118.107.9.213 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521

	经度: 114.157692
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
douyin-api.ybunx.com	IP: 172.67.139.69 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
faw.douying8.com	没有服务器地理信息.
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590
chen.ybunx.com	IP: 172.67.139.69 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.youtube.com	IP: 199.59.148.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446

120.24.233.105	IP: 120.24.233.105 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
i.ytimg.com	IP: 31.13.85.169 所属国家: Brazil 地区: Sao Paulo 城市: Sao Paulo 纬度: -23.547121 经度: -46.637184
baq.fbafb.cn	没有服务器地理信息.
dfe.hapha.cn	没有服务器地理信息.
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
43.231.0.225	IP: 43.231.0.225 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692

jsperf.com	IP: 104.16.227.18 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
noembed.com	IP: 151.101.193.91 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
34.92.95.149	IP: 34.92.95.149 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
go.aniview.com	IP: 104.96.143.45 所属国家: Austria 地区: Wien 城市: Vienna 纬度: 48.208889 经度: 16.372080
hertzen.com	IP: 104.21.65.51 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
raw.githubusercontent.com	IP: 185.199.111.133 所属国家: United States of America 地区: Pennsylvania 城市: California

	纬度: 40.065647 经度: -79.891724
cdn.plyr.io	IP: 104.26.13.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
ldy.nroom10.com	没有服务器地理信息.
html2canvas.hertzen.com	IP: 172.67.140.170 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
imasdk.googleapis.com	IP: 114.250.63.33 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.youtube-nocookie.com	IP: 31.13.88.26 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
cres.rqi564.com	IP: 149.104.35.195 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692

101.132.69.237	IP: 101.132.69.237 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
brianleroux.github.com	没有服务器地理信息.
fall.faj135.com	IP: 149.104.35.195 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
vimeo.com	IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
aomedia.org	IP: 69.171.229.11 所属国家: United States of America 地区: California 城市: Menlo Park 纬度: 37.436935 经度: -122.193604
pan.baidu.com	IP: 110.242.69.176 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
	IP: 104.21.64.1 所属国家: United States of America

npms.io	地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.h-gpro.com	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
cdn.jsdelivr.net	IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe 纬度: 32.548328 经度: -92.045235
player.vimeo.com	IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554

 URL线索

URL信息	Url所在文件
https://chen.ybunx.com/apk/app-1.1.0-3.apk	defpackage/j00.java
https://dfe.hapha.cn	defpackage/l00.java
https://api.h-gpro.com	defpackage/l00.java
https://baq.fbafb.cn	defpackage/l00.java

https://faw.douying8.com	defpackage/l00.java
https://douyin-api.ybunx.com	defpackage/l00.java
http://schemas.android.com/apk/res/android	defpackage/b0.java
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://jsperf.com/b64tests	摸瓜V2引擎
http://server/myapp/index.html	摸瓜V2引擎
https://issues.apache.org/jira/browse/CB-11522)	摸瓜V2引擎
https://html2canvas.hertzen.com >	摸瓜V2引擎
https://hertzen.com >	摸瓜V2引擎
https://cdn.jsdelivr.net/npm/workbox-cdn@5.1.4/workbox	摸瓜V2引擎
https://cdn.plyr.io/3.7.2/plyr.svg	摸瓜V2引擎
https://cdn.plyr.io/static/blank.mp4	摸瓜V2引擎
https://player.vimeo.com/api/player.js	摸瓜V2引擎
https://player.vimeo.com/video/	摸瓜V2引擎
https://vimeo.com/api/oembed.json?url=	摸瓜V2引擎
https://www.youtube.com/iframe_api	摸瓜V2引擎
https://noembed.com/embed?url=https://www.youtube.com/watch?v=	摸瓜V2引擎
https://imasdk.googleapis.com/js/sdkloader/ima3.js	摸瓜V2引擎

https://www.youtube-nocookie.com	摸瓜V2引擎
http://www.youtube.com	摸瓜V2引擎
https://i.ytimg.com/vi/	摸瓜V2引擎
https://go.aniview.com/api/adserver6/vast/	摸瓜V2引擎
https://hfive.qsxon.com	摸瓜V2引擎
https://t.me/	摸瓜V2引擎
https://t.me/\$	摸瓜V2引擎
https://pan.baidu.com/s/1wPIQE5srd_cGuPVqBWNUxw?pwd=1234	摸瓜V2引擎
https://ldy.nroom10.com:19999/nhft001	摸瓜V2引擎
https://cres.rqi564.com	摸瓜V2引擎
https://dzu541irseb11.cloudfront.net/api/v1	摸瓜V2引擎
https://fall.faj135.com/api/v1/	摸瓜V2引擎
https://120.24.233.105:16888/api/v1/	摸瓜V2引擎
https://leg.rym508.com/api/v1/	摸瓜V2引擎
https://spark.hzo732.com/api/v1/	摸瓜V2引擎
https://101.132.69.237:16888/api/v1/	摸瓜V2引擎
https://43.231.0.225:19888/api/v1/	摸瓜V2引擎

https://34.92.95.149:19888/api/v1/	摸瓜V2引擎
https://aomedia.org/emsg/ID3	摸瓜V2引擎
https://github.com/mathiasbynens/CSS.escape).	摸瓜V2引擎
https://npms.io/search?q=ponyfill.	摸瓜V2引擎
https://github.com/crypto-browserify/crypto-browserify	摸瓜V2引擎
https://img01.yzcdn.cn/vant/share-sheet-	摸瓜V2引擎
https://img01.yzcdn.cn/vant/empty-image-	摸瓜V2引擎
http://swiperjs.com\n	摸瓜V2引擎
https://github.com/indutny/elliptic/issues	摸瓜V2引擎
https://github.com/indutny/elliptic	摸瓜V2引擎
https://github.com/axios/axios.git	摸瓜V2引擎
https://github.com/axios/axios/issues	摸瓜V2引擎
https://axios-http.com	摸瓜V2引擎
https://developer.mozilla.org/fr/docs/Web/API/CustomEvent	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://brianleroux.github.com/lawnchair/),	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎

http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
sy12god@gmail.com	摸瓜V2引擎
git@github.com fedor@indutny.com	摸瓜V2引擎
solderzzc@gmail.com stefano.magrassi@gmail.com	摸瓜V2引擎

 手机线索

手机号	所在文件
-----	------

19919152923	摸瓜V2引擎
-------------	--------

✿ 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=xx, ST=xx, L=xx, O=XX, OU=xx, CN=xx.com
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-10 21:19:14+00:00
有效期至: 2052-10-26 21:19:14+00:00
发行人: C=xx, ST=xx, L=xx, O=XX, OU=xx, CN=xx.com
序列号: 0x5bd11fa1
哈希算法: sha256
md5值: 212c695387351a37d12fc12c9f5ff083
sha1值: 10ab7357e654c7aadcf939d8fb00e89350a460f0
sha256值: 7a99593b912c9c83dbe14b2b88a4032467dccd711a4ddcab90a32ffa1288189e
sha512值: 60d059161c7bdf6b02921ef06f0e7841f4fe1e66d7b14726118e906ba266fbe568fb83ab2e50bfe950e9449d93edfbf4dd006fdc4c4969c9cf281f28dbb5a0d9
公钥算法: rsa
密钥长度: 2048
指纹: e15ddf4b61a2996a92c76be11efc85caa78766ad3b7b79091983102fa12f4b7e

🔑 硬编码敏感信息

🌀 加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取

应用内通信